LAW OFFICES OF ANDREW J. BROWN
Andrew J. Brown
Brian J. Ellsworth
501 West Broadway, Suite 1490
San Diego, CA 92101
Telephone; (619) 501-6550
andrewb@thebrownlawfirm.com
briane@thebrownlawfirm.com

*Attorneys for Plaintiffs on behalf of themselves, and all others similarly situated*

BLOSSOM LAW PLLC
Rashad Blossom
301 S. McDowell Street, Ste. 1103
Charlotte, NC 28204
(704) 256-7766

*Local Counsel for Plaintiffs*

**UNITED STATES DISTRICT COURT**
**WESTERN DISTRICT OF NORTH CAROLINA**
**CHARLOTTE DIVISION**

NANCY GEORGION, SUSAN PURDY, THAN SILVERLIGHT, CHRISTINA SMITH, and DONNA WILLIAMS, *on behalf of themselves and all others similarly situated,*

Plaintiffs,

vs.

BANK OF AMERICA, N.A.

Defendant.

Case No. 3:22-cv-00618-RJC-WCM

**FIRST AMENDED CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiffs Nancy Georgion, Susan Purdy, Than Silverlight, Christina Smith, and Donna Williams (collectively, "Plaintiffs") hereby file this Class Action Complaint against Defendant Bank of America, N.A. (hereinafter "BOA" or "Defendant"), on behalf of themselves and all others similarly situated. Plaintiffs bring this action based upon personal knowledge of the facts pertaining to themselves, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

## I. NATURE OF THE ACTION

1. BOA, along with six of the nation's other large banks, created "Zelle" – an electronic payment system to compete with the wildly popular consumer payment systems such as PayPal, Venmo, and CashApp. In order to encourage and expand the use of Zelle, after it launched in 2017 BOA began embedding Zelle into every customer's online account, and aggressively advertised it to its customers as "safe," "secure," and "easy." And in a further attempt to differentiate Zelle from its competitors, BOA and Zelle contended it offered faster payments between bank accounts, allowing the transaction to occur within seconds, while Zelle also advertised it as safe and secure because it was "backed by the banks."

2. Defendant's efforts have been extraordinarily effective. Zelle is now the single most popular such platform in the U.S., processing more money than Venmo and CashApp combined.[1]

3. But Zelle is neither safe nor secure. In fact, it is a favorite mechanism for criminals and fraudsters to steal money from BOA customers for the very same reasons that BOA was able to effectively encourage its customer base to rapidly adopt it. For, unlike other peer-to-peer payment apps such as Venmo, Zelle is already integrated in the customer's online banking app and automatically connected to their bank account. Criminals can quickly, clandestinely and

[1] Forbes, "Despite A Late Start, Bank-Owned Zelle Moves More Money Than Venmo and Cash App Combined," Emily Mason, September 8, 2022, available at: https://www.forbes.com/sites/emilymason/2022/09/08/despite-a-late-start-bank-owned-zelle-moves-more-money-than-venmo-and-cash-app-combined/?sh=7c175ed89d3f (last accessed November 4, 2022).

irreversibly move money out of the BOA account once they gain access to it. As noted by Senator Elizabeth Warren, Bank of America and its cohorts "created the perfect weapon for criminals to use, and they have used it."[2]

4. Fraud that victimizes BOA's own customers through Zelle generally comes in two forms: 1) activity in which a user's checking and/or savings account is accessed by a bad actor and used to transfer a payment to another account controlled by the fraudster – referred to as "unauthorized" transactions – and 2) activity in which a user is fraudulently induced into transferring a payment to a bad actor – often referred to by BOA as "authorized" transactions.

5. BOA is of course aware that its customers are losing tens of millions of dollars every year due specifically to ***unauthorized*** transactions via Zelle. But, BOA does nothing, in large part because BOA has an enormous financial incentive to push Zelle on its customers and encourage them to use it. First, BOA is a controlling bank with an ownership stake in Zelle and profits through Zelle. Second, BOA saves millions of dollars by avoiding paying transaction fees to other competing networks. Third, BOA saves millions of dollars by reducing the amount of checks and cash transactions it is required to process. Last, BOA saves tens of millions every year by unlawfully refusing to reimburse consumers for unauthorized transactions.

6. Although BOA knows otherwise, it advertises its online and mobile banking as "safe" and "secure," and never discloses to its customers that BOA subjected each and every one of them to a high risk of fraud for unauthorized transactions by embedding Zelle into each user's account. BOA ***guarantees***,


[2] Senate Report, *Facilitating Fraud: How Consumers Defrauded on Zelle are Left High and Dry by the Banks that Created It*, By Senator Warren, October 2022.

7. Often, BOA customers are unaware of Zelle until they learn money has been stolen from their account. Victims of unauthorized transactions via Zelle, like Plaintiffs here, are left devasted after losing hundreds or thousands of dollars each time it occurs. For many customers, that money is needed to pay for rent, groceries, medicine or other necessities. Nonetheless, BOA refuses to help their customers when criminals steal money from their accounts – in spite of an unqualified ***guarantee*** and an undeniable legal obligation to do so – who have lost tens of millions of dollars through unauthorized transactions.

8. BOA is legally obligated to reimburse its customers for these losses from unauthorized transactions, but doesn't. For theft resulting from unauthorized transactions, the burden rests squarely on the shoulders of BOA to conduct a reasonable investigation of the theft and either a) reimburse their customers or b) satisfy its own burden of showing that the customer's loss was not the result of an "Unauthorized Transaction."[3] But as a matter of company-wide policy and practice, BOA does neither. BOA's "investigation" is comprised of little more than simply reviewing the payment instructions. But in the case of an unauthorized transfer (such as a hacked account or stolen phone), that is no investigation at all – the "payment instructions" are given by the fraudster himself and without authorization from the account holder. Instead, BOA places the burden on its own customers – who are victims of the fraud – to prove the fraud and refuses to reimburse them unless the consumer can prove to BOA's satisfaction that the loss qualifies as an Unauthorized Transaction. And even then, in many cases BOA still refuses to reimburse its customers.

## II. JURISDICTION

9. The Court enjoys original subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because this case arises out of violations of federal law under the EFTA, 15 U.S.C. §§ 1693, et seq. Jurisdiction of this Court arises pursuant to 28 U.S.C. §§ 1331 and 1367 for supplemental jurisdiction over the state law claims asserted herein.

[3] See, generally, 15 U.S.C. §§ 1693*, et seq.* and 12 CFR Part 1005 (Regulation E).

10. The Court also has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because (i) there is minimal diversity; (ii) Defendant is not a government entity against whom the District Court may be foreclosed from ordering relief; (iii) there are more than one hundred (100) people in the putative classes; and (iv) the amount in controversy exceeds $5,000,000, including attorneys' fees but exclusive of interest and costs.

## III. VENUE

11. Venue in this District is proper pursuant to 28 U.S.C. § 1391(b) because Defendant has its headquarters in this district, Defendant transacts business within this judicial district and at all times relevant to these claims, a substantial part of the conduct and events giving rise the causes of action against Defendant occurred in this district.

## IV. PARTIES AND NON-PARTY

12. **Plaintiff Nancy Georgion** ("Georgion") is a South Carolina citizen and resides in Central, South Carolina. She is over 70 years old and has been a Bank of America accountholder since the 1990's. She continues to maintain personal savings and checking accounts with Defendant. She has never used Zelle and was not aware of how it worked with her account(s).

13. On or about April 9, 2022, Georgion received a phone call from a person identifying themselves as a Bank of America employee who was investigating suspicious transactions to Georgion's account. During the course of the conversation, Georgion was deceived into providing account information as a means of protecting herself against the fictional suspicious transactions. Immediately thereafter she had approximately $2,000 transferred out of her checking account via Zelle. She did not initiate the transaction or authorize it in any way.

14. Georgion immediately reported the unauthorized transaction to Bank of America over the phone. The Bank of America representative told her they would investigate the claim. On May 24, 2022, Bank of America denied the claim because it asserted the investigation revealed that the transaction was processed according to the payment instructions and therefore it was not an Unauthorized Transaction. Bank of America did not provisionally credit Georgion's account

during the investigation and did not provide her with the evidence Bank of America relied upon to reach its conclusion.

15. **Plaintiff Susan Purdy** ("Purdy") is a New York state citizen and resides in Liverpool, New York. She has been a Bank of America account holder for more than 15 years. She continues to maintain personal savings and checking accounts with Defendant.

16. On or about June 29, 2022, Purdy received a text message on her phone from a recognized Bank of America (fraud department) phone number. She believed she was communicating with Bank of America and was told that she had a suspicious transfer scheduled from her checking account. Purdy was deceived into providing account login information because she believed she was protecting herself from the suspicious transfer. Immediately thereafter she had $855 transferred out of her checking account via Zelle – which was all the money in the account. She did not initiate the transaction or authorize it in any way.

17. Purdy immediately reported the unauthorized transaction to Bank of America over the phone. The Bank of America representative told her they would investigate the claim. On or about July 15, 2022, Bank of America denied the claim because it asserted the investigation revealed that the transaction was processed according to the payment instructions and therefore it was not an Unauthorized Transaction. Bank of America did not provide her with the evidence Bank of America relied upon to reach its conclusion.

18. **Plaintiff Than Silverlight** ("Silverlight") is a California citizen and resides in Lancaster, California. He is 72 years old and has been a Bank of America account holder for almost 30 years. He continues to maintain savings and checking accounts with Defendant.

19. On or about March 11, 2022, Silverlight erroneously sent a payment via PayPal to a third party. Silverlight went online in an attempt to reverse the payment and unwittingly ended up communicating with a fraudster who was impersonating PayPal. The person deceived Silverlight into providing his Bank of America account access information and the fraudster immediately began withdrawing money from Silverlight's account via Zelle. Silverlight suffered

four different transactions in varying amounts over the course of a few minutes and lost more than $3,000. He did not initiate the transaction or authorize it in any way.

20. Silverlight immediately reported the unauthorized transaction to Bank of America over the phone. The Bank of America representative told him they would investigate the claims. Thereafter, Bank of America denied the claim because it asserted the transaction was processed according to the payment instructions and therefore it was not an Unauthorized Transaction. Bank of America did not provide him with the evidence Bank of America relied upon to reach its conclusion.

21. **Plaintiff Christina Smith** ("Smith") is a Michigan citizen and resides in Bellevue, Michigan. She has been a Bank of America account holder for approximately 3 years. She continues to maintain personal savings and checking accounts with Defendant. She has never used Zelle and was not aware of how it worked with her account(s).

22. On or about March 22 and 23, 2022 an acquaintance of Smith used her phone without her permission and unbeknownst to her, to execute five different transactions transferring money from her Bank of America checking account to the acquaintance via Zelle. On March 22 there were three transactions totaling approximately $850 and on March 23 there were two more transactions totaling approximately $750. She did not initiate the transactions or authorize them in any way.

23. Smith learned of these transactions by checking her Bank of America account on her phone and discovering them within days. She immediately reported the unauthorized transactions to Bank of America by visiting her local branch. The Bank of America representative told her they would investigate the claim. Subsequently, Smith received a letter in the mail from Bank of America denying the claim because it asserted the transaction was processed according to the payment instructions and therefore it was not an Unauthorized Transaction. Bank of America did not provide her with the evidence Bank of America relied upon to reach its conclusion.

24. **Plaintiff Donna Williams** ("Williams") is a New Jersey citizen and resides in Bayonne, New Jersey. She is 69 years old and has been a Bank of America account holder for

more than 20 years. She continues to maintain personal savings and checking accounts with Defendant. She has never used Zelle and was not aware of how it worked with her account(s).

25. On or about March 25, 2022, she made a call to what she thought was Apple TV because she was having trouble with that subscription service. The person on the other end of the call told her to download an app called AnyDesk Remote. The fraudster advised her to turn on her phone's camera to show the modem was on, which she did. Within seconds, on her phone she saw money moving from her checking account. She saw him create a Zelle account for "Jacklyn" and moved money from her savings account to her checking account and then transferring that money to "Jacklyn." During this time, which was less than a couple minutes, Williams could see she was getting a call from Bank of America but somehow she was unable to answer them and they were cutoff. All told, Williams lost more than $3500 from this fraudster in what seemed to be a matter of seconds. Williams did not initiate any of the transactions or authorize them in any way.

26. Williams immediately reported the unauthorized transactions to Bank of America by telephone. She reported 3 claims in total, two on March 10 and one on March 28, 2022. The Bank of America representative told her they would investigate the claim. Williams was notified by Bank of America that they denied the claims because it asserted the transaction was processed according to the payment instructions and therefore it was not an Unauthorized Transaction.. Williams was told the first claim was deemed a "scam" which meant Plaintiff had some participation in the scheme. Bank of America did not provide her with the evidence Bank of America relied upon to reach its conclusion.

27. **Defendant Bank of America, N.A.** ("BOA") is one of the largest nationally-charted banks in the United States. BOA maintains its principle executive offices at Bank of America Corporate Center, 100 N. Tryon Street, Charlotte, North Carolina. Much of the conduct complained of herein, including the adoption and implementation of certain policies and procedures, originated or took place at the corporate headquarters.

28. **Non-Party Early Warning Services, LLC** ("Early Warning") is a privately-held financial services company owned and controlled by Bank of America, Capitol One, JPMorgan

Chase, PNC Bank, US Bank, Wells Fargo, and Truist. Its principal asset is "Zelle." Zelle is a money payment platform ("MPP"). Zelle is incorporated into BOA's online and mobile banking platform and is designed to facilitate and execute peer-to-peer ("P2P") instant payment services.

## V. FACTUAL ALLEGATIONS

### A. The Rise of Peer to Peer Payments

29. Peer to peer (P2P) payment systems, also known as money transfer apps, allow users to send and receive money from their mobile devices through a linked bank account or credit or debit card. Examples of popular P2P systems include PayPal, Venmo, Google Pay, and CashApp.

30. In the past, sending money meant using cash, mailing a check, initiating a bank or "wire" transfer, or using a debit or credit card. All of these situations were inconvenient, expensive or took time for the recipient to actually receive the money in their bank account. And they cost both the sending and receiving bank money (as well as the parties, sometimes) because each participating bank had to process these transactions.

31. With P2P payments, users can quickly send funds while keeping their bank account details private. Usually, all that is required to make a P2P payment is the recipient's user name, email, or phone number. For example, if two persons want to split a restaurant bill at the time of payment, one person can simply take out their phone, open the app, type the amount to send, enter the recipient's phone or email to find his/her account, and hit send. The money is instantly transferred and there is no processing fee. These app-based payment systems are very popular for sending money between friends to split a check, pitch in for gifts, as payment for rent to landlords, and to pay for services at the time they are performed.

32. Although P2P transactions have exploded over the past few years, P2P payments are nothing new. Venmo hit the market in 2009 as a P2P payment service and was acquired by PayPal in 2013. Venmo in particular has gained huge popularity since 2015, especially with consumers between the ages of 18-35.

33. Venmo generally does not charge users for sending or receiving money and initially was frequently used to split tabs among friends or share roommate expenses like rent and utility bills. In order to send or receive money through Venmo, users had to download an app, create an account, and link it to a bank card or banking account. Venmo initially limited the transactions to a maximum of $299 until the user verified his/her identity.

34. App use for transferring money and making payments has skyrocketed in the last 10 years. In 2016, Venmo processed over $17 billion in payments and processed almost $7 billion in the first quarter of 2017. Zelle's growth continues, rising to $490 billion in payments in 2021, more than double Venmo's P2P volume.[4] Zelle has transferred $1.5 trillion since 2017.

**B. Zelle Is Created And Marketed To Compete With P2P Systems**

35. To compete with Venmo and other P2P apps, a consortium of the largest banks teamed up to launch their own money transfer app called "Zelle." While Zelle is owned by Early Warning Service ("EWS"), EWS is owned, operated, and controlled by seven of the largest banks in this country, including Defendant Bank of America, N.A.

36. Launched in June 2017, Zelle is a P2P payment service created to compete with other electronic payment services like Venmo. Zelle lets banks handle electronic transfers without paying any fees to third parties.

37. With Venmo and other P2P apps gaining so much popularity, Zelle and BOA recognized that it would be difficult to compete with Venmo, et al., and convince users to switch to using Zelle. Therefore, Zelle differentiated itself from Venmo by marketing Zelle as "faster" and "safer" than its competition. Zelle advertisements emphasized its security and safety, because it is "backed by the banks." [5]

---

[4] American Banker, "Can Zelle change the narrative around P2P fraud?," Kate Fitzgerald, March 9, 2022, available at: https://www.americanbanker.com/payments/news/can-zelle-change-the-narrative-around-p2p-fraud (last accessed November 4, 2022)

[5] Tech Crunch, "Zelle p2p payments push to compete with Venmo now has 19 US FI backers" Natahsa Lomas, (October 24, 2016), available at: https://techcrunch.com/2016/10/24/zelle-p2p-payments-push-to-compete-with-venmo-now-has-19-us-fi-backers/ (last accessed November 4, 2022).

38. For example, in a 2018 television commercial, Zelle hired performer Daveed Diggs from the Broadway show Hamilton to rap: "You can send money safely cause that's what it's for / It's backed by the banks so you know it's secure." In another commercial with Daveed Diggs, Zelle similarly advertised that is "safe" and "backed by the banks."[6]

39. Zelle's CEO also publicly touted its safety and faster payments. Zelle offers a "faster payments network that will revolutionize how U.S. consumers and businesses send and receive money " said Paul Finch, then CEO of EWS. He announced that Zelle " will change how money moves, empowering millions of consumers with a faster, safer way to send and receive payments within the security of their financial institution." [7]

40. Likewise, Lou Anne Alexander, group president of payments for Early Warning stated in an interview: "As I've said, Matt, consumers know two things about the way that they pay. They do not pay to pay, and it's really difficult to get consumers out of their current payment behavior. Just think about it -- you probably pay your landlord in the very same way; you probably pay for your groceries in a very different way than you pay your babysitter. As we're focusing on changing consumer behavior, we're having great success in helping customers understand that it can be fast, and it can be easy. But we also have to help them understand it also can be safe for them." [8]

41. To gain users, Zelle also marketed to an older demographic that may not be comfortable using Venmo due to safety or security concerns. Melissa Lowry, Early Warning's vice president of marketing and branding, stated they are targeting an older age demographic. She noted that "This group has a high trust in their banks," so Zelle "wants to remind these consumers

[6] WRAL News, Zelle Fraud protection: What You Need to know Before Transferring Funds, May 1, 2018) available at: https://www.wral.com/zelle-fraud-protection-what-you-need-to-know-before-transferring-funds/17523584/ (last accessed November 4, 2022).

[7] Zelle Press Release, October 24, 2016, available at: https://www.zellepay.com/press-releases/early-warning-announces-zelle-network (last accessed November 3, 2022)

[8] Fox Business News, Bank Earnings and Getting to Know Zelle. Matt Frankel, available at: https://www.foxbusiness.com/markets/bank-earnings-and-getting-to-know-zelle (last accessed November 4, 2022)

that money transfer isn't just for splitting a restaurant tab, it can also be used for splitting a payment on kids' sports uniforms or grocery store bills, Lowry said. "That demographic had been a bit ignored in the (P2P) category." *Id.*

42. This marketing strategy worked by attracting an older demographic that trusted Bank of America. "76% of Gen X and 74% of Baby Boomers also said that offered through their financial institution was the key reason that they would trial P2P payments." *Id.*

43. But Zelle is different from other digital payment systems such as PayPal, Google Pay, or Venmo in several important respects. ***First***, with Zelle, the transfer goes ***immediately*** from bank account to bank account – there is no entity holding onto the money while the transaction is verified or before it's collected by the recipient. Zelle doesn't hold the money for any period of time. Instead, the money transfers immediately from a BOA customer's bank account to the recipient's bank account.[9]

44. Secondly, unknown to many BOA customers, Zelle is automatically integrated in the customers' BOA account. This allows criminals to instantly transfer money via Zelle from BOA customers who are not even aware of the Zelle feature imbedded in their online accounts.

### C. Unknown To Many BOA Customers, Zelle Is Embedded In Their Accounts And "Always On" – It Cannot Be Removed Or Disabled

45. BOA has embedded Zelle in each and every Bank of America online and mobile account. It cannot be removed by the customer; nor can it be disabled. According to Brian Moynihan, CEO of BOA, Zelle is "always on."[10]

[9] La Times, Do you use Zelle? Here's how to spot increasingly common scams. (Oct. 7, 2022) Jon Healey, available at: https://www.latimes.com/business/technology/story/2022-10-07/zelle-banks-may-not-cover-the-losses-from-scams (last accessed Nov 3, 2022).

[10] Zelle Press Release, October 24, 2016. Available at: https://www.zellepay.com/press-releases/early-warning-announces-zelle-network (last accessed November 3, 2022).

46. Being integrated in the banking platform offered a big competitive advantage for Zelle. "There's no need to download an additional app, it's right there in the trusted financial institution, online banking or mobile banking app that I currently use." [11]

47. "One of Zelle's unique characteristics is that it is embedded within the online and mobile banking experience of individual network banks," said the spokesperson. "That means customers never have to leave the safety of their financial institution to make a payment. There is never a need for a customer to provide an account number to a third party app, which is one very effective way for Zelle users to protect their identity and payments."

48. Bank of America does not offer customers a way to delete or disable the Zelle function. BOA does not provide any means, or instructions, on how to turn Zelle off or prevent fund transfers via Zelle. By design, BOA customers simply cannot avoid the unauthorized transfers via Zelle even if they wanted to.

### D. BOA and Zelle Make It Easy To Steal From Customer BOA Accounts

49. Zelle and BOA created the perfect weapon for criminals to use and they have used it. The National Consumer Law Center has described Zelle as "a dangerous payment system" and it has become the preferred tool for criminals.[12]

50. Because it is already embedded into the BOA account, and the money transfer is immediate, criminals can easily and quickly transfer money out of a BOA bank account. In fact, criminals have targeted BOA customers precisely because Zelle is already integrated in their

[11] Bank Earnings and Getting to Know Zelle, April 17, 2019, available at: https://www.foxbusiness.com/markets/bank-earnings-and-getting-to-know-zelle (last accessed November 3, 2022).

[12] See fn. 26. "95% of the shut-off scams requested payment through Zelle."

account and they can quickly and irreversibly move money out of the account once they gain access.[13] And it is costing BOA customers hundreds of millions of dollars.[14]

51. Nearly 18 million people have been victims of "widespread fraud" on money transfer apps, according to a letter sent in late April of 2022 to Zelle by U.S. Senators Elizabeth Warren of Massachusetts, Robert Menendez of New Jersey and Jack Reed of Rhode Island. Criminals have turned to Zelle as their favorite service because transfers are immediate and unrecoverable, and a fraudster can become a Zelle user (and money transfer recipient) without revealing their true identity.

52. Led by Idaho Attorney General Lawrence Wasden and Oregon Attorney General Ellen Rosenblum, a bipartisan coalition of thirty-three (33) attorneys general wrote the Consumer Financial Consumer Protection Bureau ("CFPB"), calling for stronger consumer safeguards for money sharing platforms and apps like Zelle. The letter, written in response to the CFPB's request for comments on its inquiry into "Big Tech Payment Platforms," noted a rise in complaints against popular payment apps including Zelle. The letter highlighted that: "[m]any consumers have been scammed out of hundreds or thousands of dollars by other users of these payment platforms [like Zelle]. Scammers are attracted to real-time payment platforms, in large part, because they do not need to reveal their true identity to set up an account" (emphasis added). [15]

53. Criminals can transfer money out of BOA's customer accounts using Zelle by hacking their accounts or phones, obtaining access to their phone, or even tricking customers into providing their login information.

---

[13] NBC News, "Instant Fraud, Consumers See funds disappear in Zelle account scam" Vicky Nguyen, Did Martinez, Joe Enoch, and Michelle Tak (June 11, 2019) available at: https://www.nbcnews.com/business/consumer/instant-fraud-consumers-see-funds-disappear-zelle-account-scam-n1015736 (last accessed November 3, 2022)

[14] In the period between January 2021 and September 2022, Bank of America customers reported 81,797 cases of unauthorized transactions, totaling $125 million. See fn. 2.

[15] Attorneys General Letter dated December 20, 2021 to CFPB Director Rohit Chopra, regarding "Request for Comments Big Tech Payment Platforms" Docket No CFPB-2021-0017.

54. For example, one BOA customer complained after he lost his entire savings after his phone was hacked. The criminals even deposited fake checks into the account to withdraw more funds. Bank of America refused to return his money, despite what appeared to be obvious fraud and unauthorized transactions. [16]

55. Sometimes criminals use a phishing email or phone call that appears to be from BOA itself, tricking consumers into entering their bank ID and password into a fraudulent website. Once a fraudster gains this information, they have unfettered access to transfer funds from the account immediately using Zelle.

56. And hackers have figured out how to defeat any text-message-based authentication for Zelle transfers. Either they trick victims into divulging authentication codes, in a phone call, or they intercept the messages electronically. In the past, criminals also have cloned phones, or simply changed the cell phone number associated with an account so the message is directed at a phone they control. [17]

57. Ken Otsuka, a senior risk consultant at CUNA Mutual Group, an insurance company that provides financial services provides the example of one such scam. Otsuka said a fraudster may call from a number spoofed to look like its coming from your bank, so suspicious customers will look up the number and believe it is indeed their bank calling. Next, the fraudster may inform you that there appear to be some fraudulent transactions on your account and ask: "Before I get into the details, I need to verify that I'm speaking to the right person. What's your username?" "In the background, they're using the username with the forgot password feature, and that's going to generate one of these two-factor authentication passcodes," Otsuka said. "Then the fraudster will say, 'I'm going to send you the password and you're going to read it back to me over

[16] CBS News, "Zelle blames after Lexington teen'sbank account cleaned out my money transfer hackers" Cheryl Fiandaca, (Mayo 10, 2022), available at: https://www.cbsnews.com/boston/news/zelle-hackers-scammers-theft-bank-of-america-cogan-lawler/ (last accessed November 4, 2022).

[17] Bob Sullivan, Zelle Crminial took $23k from elderly victim; (BofA (initially) wouldn't give it back", (August 26, 2019), available at: https://bobsullivan.net/cybercrime/zelle-criminal-took-23k-from-elderly-victim-bofa-initially-wouldnt-give-it-back/ (last accessed November 4, 2022).

the phone.'" The fraudster then uses the code to complete the password reset process, and then changes the victim's online banking password. The fraudster then has unfettered access to use Zelle to transfer the victim's funds.[18]

58. An important aspect of this scam is that ***the fraudsters never even need to know or phish the victim's password***. By sharing their username and reading back the one-time code sent to them via email, the victim is unwittingly allowing the fraudster to reset their online banking password. Normally, gaining access to your online account would not result in immediate financial harm. However, with Zelle embedded, the fraudster can immediately drain the bank account.

59. Many BOA customers have never heard of Zelle and never knew that it was embedded into their account. Osaka noted that "Members don't have to request to use Zelle. It's just there, and with a lot of members targeted in these scams, although they'd legitimately enrolled in online banking, they'd never used Zelle before." *Id*. Like Plaintiffs Georgion and Smith, many customers first learn of BOA's Zelle feature only after their money is gone.

60. There are literally thousands of examples. For instance, criminals stole nearly $23,000 from an 86-year-old New Hampshire woman, who had never heard of Zelle, draining her Bank of America checking and savings accounts. Criminals were able to complete eight separate $2,499 withdrawals from the victim's account — $1 below BOA's daily transfer limit - calling into question the bank's ability or willingness to spot obvious Zelle fraud. The bank denied her dispute of the fraudulent charges for months, until a reporter got involved and BOA quickly reversed and refunded the money.[19]

61. One BOA customer noted that "It's like the banks have colluded with the sleazebags on the street to be able to steal." [20]

---

[18] "The 'Zelle Fraud' Scam: How it works, How to fight back" November 19, 2021, https://krebsonsecurity.com/2021/11/the-zelle-fraud-scam-how-it-works-how-to-fight-back/comment-page-1/ (last accessed November 4, 2022).
[19] See fn. 17.
[20] https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html

### E. Bank of America Markets Zelle To Its Customers As Safe and Secure

62. Like Zelle, BOA makes repeated promises on its website, app, and elsewhere that Zelle is a "fast, safe and easy way to send and receive money," and that its online banking offers a "secure, convenient experience." [21]

63. First, BOA's digital banking webpage peddles the security and safety of its app to consumers. "Want a secure, easy way to bank on the go? Download the app today. It's safe, simple and convenient." BOA claims that its app delivers "the most convenient and secure experience." [22]

64. Likewise, BOA promotes Zelle and its security and safety. "Zelle is an always-on, easy to use mobile payment capability that gives our customers one more secure, convenient way to stay connected and live their financial lives," said Brian Moynihan, chief executive officer of Bank of America. [23]

65. BOA advertised that Zelle "will provide consumers a faster, easier way to send and receive payments in minutes without leaving the security of their own financial institution."[24]

66. BOA also recognized that it could reach an older population that may not be comfortable using Venmo to send money. Because Zelle is sponsored by and connected to their banks, Alexander said users should feel more comfortable using it for larger transactions and for a broader array of uses.

### F. BOA Does Not Disclose To Its Customers The Risks Posed By Zelle

67. BOA knows that Zelle is not secure and that fraud and unauthorized transactions are overwhelming its own customers. Consumers began complaining about unauthorized

---

[21] https://www.bankofamerica.com/online-banking/; https://www.bankofamerica.com/online-banking/mobile-and-online-banking-features/send-receive-money/

[22] https://promotions.bankofamerica.com/digitalbanking/mobilebanking.

[23] See fn. 10.

[24] Money Magazine, "America's Biggest banks Just Rolled Out Their Venmo Killer", Lucinda Shen (Feb 22, 2017), available at: https://money.com/jpmorgan-big-banks-venmo-zelle-bank-of-america-citigroup/ (last accessed November 4, 2022)

transactions and money being stolen out of their account shortly after Zelle was launched and embedded into BOA's customers' accounts in 2017.

68. By 2018, there were numerous news reports, including a NY Times report of BOA customers losing money after being scammed or hacked through the use of Zelle.[25] And of course, BOA gets tens of thousands of reports from its own customers every year, which it claims to "investigate."

69. BOA is also painfully aware that bad actors are routinely hacking into consumers accounts, phones, or tricking its customers into providing their account information and often setting set up the Zelle account embedded into each BOA account to steal money.

70. But even after users complain about funds being stolen from their accounts through the embedded Zelle feature, BOA frequently does nothing. Instead, BOA continues to promote both its online banking and Zelle as "secure" and "safe". Yet nowhere in Defendant's marketing do they warn potential BOA customers of the risks of being scammed by persons impersonating their banks due to Zelle.

71. Consumers are often not aware of Zelle. And even if they know of it and use it, consumers are not aware that money transfer transactions with Zelle differ from other similar platforms. Unbeknownst to most BOA users, the Zelle network has become a preferred tool for fraudsters to victimize BOA customers.

72. In fact, due to the myriad security risks Zelle presents, security experts advise consumers not to use Zelle at all.[26] But BOA does not offer a way for consumers to delete Zelle from their online banking account or mobile app in order to protect themselves.

---

[25] See, e.g. https://www.nytimes.com/2018/04/22/business/zelle-banks-fraud.html ; See also, https://www.nbcdfw.com/news/local/consumers-say-their-bank-accounts-were-hacked-through-zelle/2054119/ .

[26]Detroit Free Press "DTE Impersonators Drained Rochester Hills Woman's Checking Accounting Using Zelle App", Tompor, Susan (June 30, 2022),available at: https://www.freep.com/story/money/personal-finance/susan- tompor/2022/06/30/utility-shutoff-scam-stole-cash-via-zelle/7714138001/ (last accessed Sept. 21, 2022)

73. "Scammers go where it's easy to get the money. Zelle is their current mechanism to drain consumer accounts," warned Ed Mierzwinski, PIRG Education Fund's senior director of federal consumer programs. "The scammers are taking advantage of consumers because the banks are letting them," Mierzwinski said. "My basic advice is don't use these apps." *Id.*

### G. BOA Specifically Promised Security, Protection And Reimbursement From Unauthorized Transfers

74. BOA advertises that "Bank of America's award-winning Online Banking service incorporates industry-leading safety features that give you greater security and peace of mind as you manage your money." [27]

75. Bank of America prominently displays that it ***guarantees*** customers security on the online and mobile bank website.


76. BOA's website further promises its customers that: "Our Consumer ***Online and Mobile Banking Guarantee*** means that ***you are not liable for unauthorized transfers*** or bill payments made via Online or Mobile Banking if reported promptly."

77. BOA's website is full of promises of security, guarantees, and statements like "Your security is our top priority." For instance, BOA promises:

**" Convenient, secure banking from almost anywhere"[28]**

**"You're never liable for unauthorized purchases or transactions—as long as they're reported promptly"[29]**

---

[27] https://www.bankofamerica.com/security-center/online-mobile-banking-privacy/online-banking-security/ (last accessed November 4, 2022).

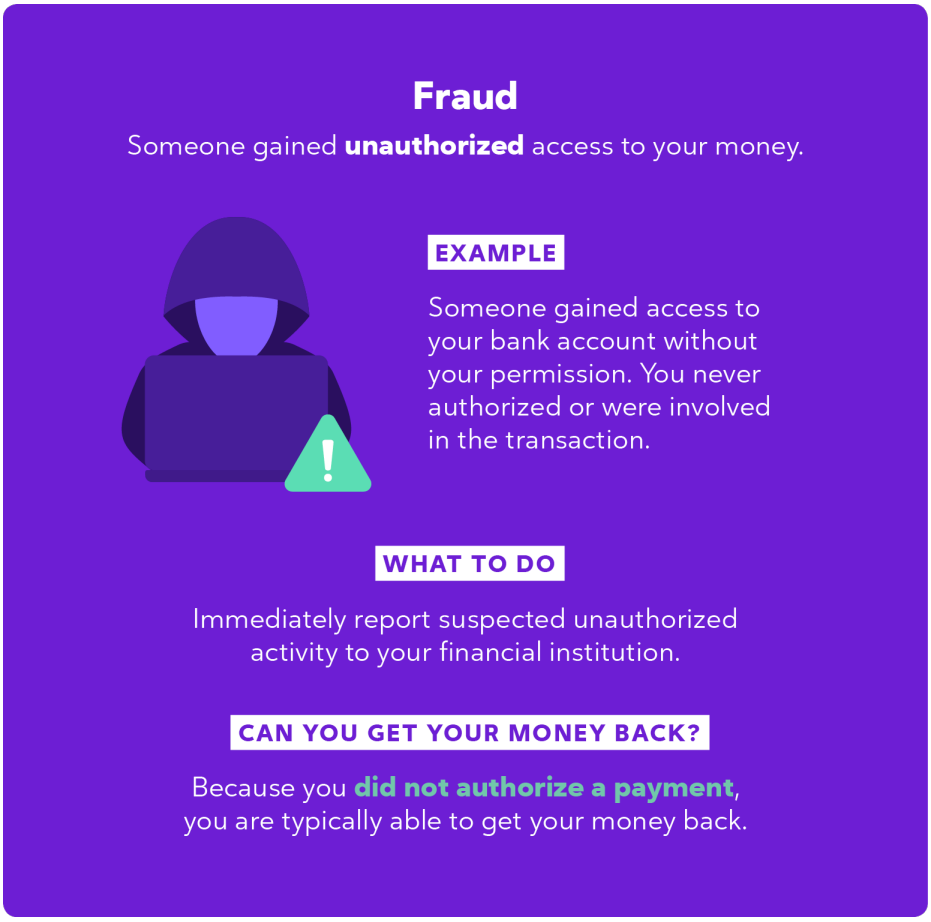
[28] https://www.bankofamerica.com/online-banking/mobile-and-online-banking-features/overview/?request_locale=en_US

[29] https://www.bankofamerica.com/security-center/overview/

And elsewhere, BOA promises:

> **You can confidently use Online or Mobile Banking—we guarantee that you will not be liable for fraudulent transactions when reported promptly and we will help keep your information safe.**[30]

78. Similarly, Zelle's website informs users that consumers should be able to get their money back from BOA when they did not authorize the transaction**.**




79. BOA's Online Banking Service Agreement also repeatedly promises users that, if they timely report fraud, that they will not be liable ***at all*** for fraudulent transfers, without limitation. ***BOA's Agreement even notes that this may provide more protections than the EFTA***.

> B. Limitation of Liability for Online Banking Transactions
>
> Tell us at once if you believe your Online Banking password has been compromised or if someone has transferred or may transfer money from your account without your permission.

[30] https://www.bankofamerica.com/online-banking/mobile-and-online-banking-features/

> The best way to minimize your loss is to call us immediately. The unauthorized use of your Online Banking services could cause you to lose all of your money in your accounts, plus any amount available under your Balance Connect™ overdraft protection service.
>
> ***You will have no liability for unauthorized transactions if you notify us within 60 days after the statement showing the transaction*** has been sent to you (or 90 days if the transaction was from an account maintained at another financial institution). If you do not, you may not get back any of the money you lost from any unauthorized transaction that occurs after the close of the 60-day period (or 90 day period if the transaction was from an account maintained at another financial institution), if we can show that we could have stopped the transaction if you had notified us in time. If a good reason (such as a long trip or hospital stay) kept you from telling us, we may extend the time periods.
>
> If you give your User ID and password and grant authority to make transfers to a person who exceeds the authority given, you are responsible for all transactions that person performs unless you notify us that the transfers by that person are no longer authorized. Transactions that you or someone acting with you initiates with fraudulent intent are also authorized transactions.
>
> ***Note: These liability rules are established by Regulation E, which implements the federal Electronic Fund Transfer Act and does not apply to business accounts. Our liability policy regarding unauthorized Online Banking transactions on consumer deposit accounts may give you more protection, provided you report the transactions promptly.*** Also, the state law applicable to your account may give you more time to report an unauthorized transaction or may give you more protection.

80. Moreover, the terms provide that it will conduct a reasonable investigation if a consumer timely reports any errors (including unauthorized transfers), will credit the consumer's account within 10 days, and will provide the customer with the "documents" used in the investigation:

> We will determine whether an error occurred within 10 business days after we hear from you, and we will promptly correct any error we have made. If we need more time, however, we may take up to 45 days to investigate your complaint or question. In this case, we will provisionally credit your account within 10 business days for the amount you think is in error, so that you have the use of the money during the time it takes us to complete our investigation. If we ask you to put your complaint or question in writing, and we do not receive your letter in 10 business days, we reserve the right not to provisionally credit your account. For errors involving new accounts, we may take up to 90 days to investigate your complaint or question and up to 20 business days to provisionally credit your account.

81. We will tell you the results within 3 business days after we complete our investigation. If we conclude there was no error, we will send you a written explanation. You may request copies of the documents that we used in our investigation.

82. BOA routinely violates each of these promises – and its legal obligations under the EFTA and Regulation E – as a matter of company policy.

83. BOA also falsely tells consumers that it will protect users by verifying the identity of the person receiving the money through Zelle:

> In most cases, when you are sending money to another user, the transfer will occur in minutes; however, there are circumstances when the payment may take longer. For example, in order to protect you, us, *Zelle* and the other Network Banks, we may need additional time to verify your identity or the identity of the person receiving the money. During this period, and in any other circumstance when we need additional time to verify the transfer details, a hold will be placed on your account for the amount of the transfer.

### H. BOA Does Not Refund Customers For Unauthorized Transactions

84. Bank of America's CEO stated under oath at a Senate hearing that Bank of America refunds consumers for unauthorized transactions.[31] Mr. Moynihan testified that "When users do submit claims, the bank investigates thoroughly and provides appropriate customer compensation consistent with its regulatory obligations, and in some cases beyond those obligations consistent with bank policy."[32] However, this is simply false most of the time, and as a matter of company policy at BOA.

85. In the period between January 2021 and September 2022, BOA customers reported 81,797 cases of unauthorized transactions, totaling $125 million. BOA refunded only $56.1 million of these claims – less than 45% of the overall dollar value of claims made in that time. [33]

86. Despite promising consumers that they won't be liable for unauthorized transactions, despite knowing that Zelle allows criminals to easily make unauthorized transfers out of customers accounts, and notwithstanding that BOA failed to notify consumers of this risk of

---

[31] In response to the question: "Will you commit today to fight fraud on the Zelle platform by giving your customers their money back?" Mr. Moynihan answered: "We reimburse today for unauthorized transactions and like Mr. Diamond said we do send out notices and everything" United States Senate Hearing, Committee on Banking, Housing & Urban Affairs, September 22, 2022.

[32] Written Statement of Brian Moynihan, Chairman and CEO Bank of America, Before the Committee on Banking, Housing & Urban affairs, United States Senate, September 22, 2022.

[33] *Facilitating Fraud: How Consumers Defrauded on Zelle are Left High and Dry by the Banks that Created It*, By Senator Warren, October 2022.

Zelle and online banking, BOA still refuses to refund its customers for unauthorized transactions resulting in part from BOA's very own conduct.

87. BOA's practices, policies and procedures do not comply with the promises made to customers, and they do not comply with Federal law.

## I. Electronic Funds Transfer Act, 15 U.S.C. § 1693 *et seq.*

88. Bank of America is required under the Electronic Fund Transfer Act to repay customers when funds are illegally taken out of their account without authorization.

89. Frequently, and as a matter of policy and practice, BOA initially denies the claims for unauthorized transactions. Instead, BOA requires the consumer to "request an additional review" after being rejected, before BOA considers refunding the stolen money.[34]

90. In enacting the EFTA, Congress found that the use of electronic systems to transfer funds provides the potential for substantial benefits to consumers. 15 U.S.C. § 1693(a). Congress' purpose in enacting the EFTA was to "provide a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund and remittance transfer systems." Id. § 1693(b).

91. "The primary objective of [the EFTA] is the provision of individual consumer rights." *Id.* In response to the EFTA, the Federal Reserve Board of Governors passed Regulation E to implement that statute. BOA and other banks are bound by the EFTA and Regulation E.

92. The EFTA and Regulation E apply to electronic fund transfers that authorize a financial institution to debit or credit a consumer's account. 12 C.F.R. § 1005.3(a). Recent CFPB guidance on ***unauthorized*** Electronic Fund Transfers ("EFTs") indicates P2P payments are EFTs, such that transactions made with Zelle will trigger "error resolution obligations" on BOA to protect consumers from situations where they are fraudulently induced and requested by a third party to provide their account information that results in unauthorized debits from their accounts.[35]

---

[34] *The New York Times*, "Zelle, the Banks' Answer to Venmo, Proves Vulnerable to Fraud" Stecey Cowley, (April 22, 2018), https://www.nytimes.com/2018/04/22/business/zelle-banks-fraud.html

[35] Consumer Financial Protection Bureau, Electronic Fund Transfers FAQs, https://www.consumerfinance.gov/compliance/compliance-resources/depositaccounts-

93. Under the EFTA, an unauthorized electronic fund transfer is an electronic fund transfer from a consumer's account "initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit."

94. The Federal Deposit Insurance Corporation ("FDIC") issued a report in March 2022 finding that Regulation E's "liability protections for unauthorized transfers apply even if a consumer is deceived into giving someone their authorization credentials."[36]

95. Under Regulation E, if the consumer alleges that there has been an unauthorized transfer, the consumer's financial institution ***must*** investigate and determine if the allegation is true, correcting any unauthorized transfer that occurred. Reg. E, 12 C.F.R. § 1005.11(c)(1) [§ 205.11(c)(1)].

96. If a consumer alleges that an EFT is unauthorized, ***the burden of proof is on the financial institution*** to show that it was authorized or that the conditions for consumer liability have been met. But the extent of the consumer's liability is determined solely by the consumer's promptness in notifying the financial institution. "Other factors ***may not be used*** as a basis to hold consumers liable."[37]

97. Consumer negligence therefore plays no role in determining the consumer's maximum liability. An example of consumer negligence could be when someone writes a PIN on the debit card and there is an unauthorized EFT through use of the debit card. Despite the consumer's negligence, which facilitated the unauthorized electronic fund transfer, the consumer's liability is totally unaffected.[38]

---

resources/electronic-fund-transfers/electronic-fund-transfersfaqs/#financial-institutions-2 (last accessed October 28, 2022)

[36] FDIC, Consumer Compliance Supervisory Highlights Federal Deposit Insurance Corporation (March 2022), available at: https://www.fdic.gov/regulations/examinations/consumer-compliance-supervisory-highlights/documents/ccs-highlights-march2022.pdf (last accessed October 28, 2022).

[37] Reg. E, Official Interpretations § 1005.6(b)-3 [§ 205.6(b)-3]. Consumer Fin. Prot. Bureau, CFPB Consumer Laws and Regulations: Electronic Fund Transfer ACT 23 (Oct. 2013), *available at* www.consumerfinance.gov (CFPB Supervision and Examination Manual; original emphasis)

[38] Reg. E, Official Interpretations § 1005.6(b)-2 [§ 205.6(b)-2].

98. The bank is also liable to the consumer if it does not conduct a good faith investigation of the claim, rejected the claim despite not having a reasonable basis to do so, or unreasonably failed to draw from the evidence that no error had occurred. 15 U.S.C. § 1693f(e).

99. The bank's efforts to investigate must be "reasonable" in light of available evidence and the consumer's report of the error. The financial institution must review any relevant information within the institution's own records for the particular account." Although the extent of the investigation "may vary depending on the facts and circumstances . . . a financial institution may not limit its investigation solely to the payment instructions where additional information within its own records . . . could help to resolve a consumer's claim." The official interpretation includes a list of examples of the type of information that a financial institution might review, including "[a]ny other information appropriate to resolve the claim." [39]

100. Importantly, when there is an agreement between a third party and the banking institution, the bank ***must*** extend its investigation beyond its own records.[40] Here, BOA has an agreement with Zelle and probably the recipient's bank to provide transactions via the Zelle network, and as a result BOA is required to examine those third-party records during an investigation.

101. BOA repeatedly and routinely fails to follow these mandatory requirements as a matter of practice and policy. For if BOA had conducted reasonable investigations and analyzed these records, it would see clear evidence of criminal activity and fraud and could not deny reimbursement of most of the unauthorized transactions it routinely denies.

102. Instead, BOA limited its investigation to the payment instructions. BOA told Plaintiffs and class members that that the transfers were "completed according to the instructions you provided to us." Therefore, "we're unable to approve your recent claim."

103. BOA ignored that Plaintiffs and class members stated they did not initiate or authorize the transactions and that the transfer was a result of fraud, hacked accounts, and stolen

[39] Reg. E, Official Interpretations § 1005.11(c)(4)-5 [§ 205.11(c)(4)-5].
[40] Reg. E, Official Interpretations § 205.11(c)(4), 12 C.F.R. § 205, Supp. I.

phones. Limiting the investigation to a review of the payment instructions is not a reasonable investigation where the consumer alleges the transfer was unauthorized. In that instance, the fraud itself was the Unauthorized Transaction – the payment instructions came from the fraudster himself.

104. Upon information and belief, BOA intentionally determined that unauthorized transfers of funds via Zelle of Plaintiffs and Class Members were not in error due to, at least in part, the Bank's financial self-interest as a stakeholder in Zelle, and to avoid its liability to Plaintiffs and other Class members for the unauthorized transfers pursuant to Regulation E.

105. If there was any confusion as to whether Plaintiffs' experiences constitute an unauthorized transfer, it was made clear by the CFPB in a compliance aid issued on June 4, 2021.[41] The CFPB stated: when a consumer is fraudulently induced into sharing account access information with a third party, and a third party uses that information to make an EFT from the consumer's account, the transfer is an unauthorized EFT under Regulation E.

> For example, the Bureau is aware of the following situations where a third party has fraudulently obtained a consumer's account access information, and thus, are considered unauthorized EFTs under Regulation E: (1) a third-party calling the consumer and pretending to be a representative from the consumer's financial institution and then tricking the consumer into providing their account login information, texted account confirmation code, debit card number, or other information that could be used to initiate an EFT out of the consumer's account, and (2) a third party using phishing or other methods to gain access to a consumer's computer and observe the consumer entering account login information. EFTs stemming from these situations meet the Regulation E definition of unauthorized EFTs.

[41] Consumer Financial Protection Bureau, Electronic Fund Transfers FAQs, at Errors Resolution: Unauthorized EFTs, Question 5. https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/

106. Defendant was aware of these schemes and the CFPB guidance, but continued denying claims that were substantially similar to the schemes described by the CFPB.

107. Bob Sullivan, a journalist and NY Times best seller, wrote: "I've since heard countless stories about victims getting the wrong advice from banks, who sometimes flat-out refuse to honor legitimate Regulation E disputes that should lead to consumers being "refunded" money stolen through unauthorized transfers. This story is important to me because it puts quite a human face on these victims. It gives me a chance to wonder why banks have gotten away with it so long, and why regulators haven't done more to fix this."

108. BOA's practices and policies of denying a claim without performing a reasonable investigation are illustrated by the Plaintiffs experiences, as well as numerous instances in which the bank only investigated the claim after being contact by a news reporter. After denying a consumer's claim, and once contacted by a journalist, BOA would then investigate the claim and refund the money "based on our additional research and information."[42] For example, hackers stole nearly $23,000 from an 86-year-old woman, by completing 8 separate $2,4999 withdrawals from her account via Zelle. $1 below the daily transfer limit, calling into question the bank's ability to spot obvious fraud. The bank refused to refund the unauthorized transactions, until being contact by a journalist.[43]

109. BOA created a system and adopted policies and procedures that treated Zelle transfers differently than other EFTs. For example, one consumer had his digital wallet accessed by a criminal that ran up charges on his credit card, took out cash at an A.T.M. and used Zelle to make three transfers totaling $2,500. When he filed fraud reports, the bank quickly refunded his

[42] "When Customers Say Their Money Was Stolen on Zelle, Banks Often Refuse to Pay", *The New York Times*, Stacy Cowley and Lananh Nguyen (June 20,2022) available at: https://www.nytimes.com/2022/06/20/business/zelle-money-stolen-banks.html (last accessed 10/31/2022); "Fraud is Flourishing on Zell. The Bank Say It's Not Their Problem", *The New York Times*, Stacy Cowley and Lananh Nguyen, March 6, 2022, available at: https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html (last accessed October 31, 2022).

[43] https://bobsullivan.net/cybercrime/zelle-criminal-took-23k-from-elderly-victim-bofa-initially-wouldnt-give-it-back/ (last accessed October 31, 2022).

cash and credit card losses. But it denied his claims for the Zelle thefts, saying the transactions were validated by authentication codes sent to a phone that had been previously used for that account. Bank of America was essentially saying that the Zelle transactions were authorized — even if his phone was stolen. Only after being contacted by the New York Times did BOA further "investigate" the claim and refund the money.[44]

110. Regulation E also requires the bank to report the results of its investigation to the consumer – which includes a written explanation of the institution's findings and the consumer's right to request the documents that the institution relied upon in making its determination. [45] As evidenced by the experiences of Plaintiffs, BOA does not comply with this obligation either.

111. On numerous occasions, when consumers notified BOA about suspected errors regarding the Zelle transfers that were unauthorized, BOA denied the claim within 10 days and informed Plaintiffs and class members that "as a courtesy, we're researching your inquiry with the other party" and it "may take up to 45 calendar days." In truth, BOA did not perform a reasonable investigation prior to denying the consumer's claim and did not a reasonable basis for doing so. Moreover, BOA employed this strategy to around the EFTA's requirement to provisionally credit the consumer's account. By doing so, BOA effectively allowed itself more than 10 days to investigate the claim without provisionally crediting the consumers account within 10 days.

## VI. CLASS ALLEGATIONS

112. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated.

---

[44] See fn. 42.

[45] Reg. E, 12 C.F.R. § 1005.11(d)(1) [§ 205.11(d)(1)]; *Bisbey v. D.C. Nat'l Bank*, 793 F.2d 315 (D.C. Cir. 1986) (bank liable when it provided oral explanation and did not inform consumer of right to request documents). Reg. E, Official Interpretations § 1005.11(d)(1)-1 [§ 205.11(d)(1)-1]. "If an institution relied on magnetic tape it must convert the applicable data into readable form, for example, by printing it and explaining any codes." *Id*

113. Each of the Plaintiffs is a member of and seeks to represent a Nationwide Class, pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), defined as:

> All Bank of America customers within the United States whose BOA consumer bank accounts were debited via one or more unauthorized transactions using Zelle and were not fully reimbursed by BOA.

114. Plaintiff SILVERLIGHT is a member of and seeks to represent a California state Sub-Class, pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), defined as:

> All Bank of America customers residing in California whose BOA consumer bank accounts were debited via one or more unauthorized transactions using Zelle and were not fully reimbursed by BOA.

115. Plaintiff GEORGION is a member of and seeks to represent a South Carolina state Sub-Class, pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), defined as:

> All Bank of America customers residing in South Carolina whose BOA consumer bank accounts were debited via one or more unauthorized transactions using Zelle and were not fully reimbursed by BOA.

116. Plaintiff PURDY is a member of and seeks to represent a New York state Sub-Class, pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), defined as:

> All Bank of America customers residing in New York whose BOA consumer bank accounts were debited via one or more unauthorized transactions using Zelle and were not fully reimbursed by BOA.

117. Plaintiff WILLIAMS is a member of and seeks to represent a New Jersey state Sub-Class, pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), defined as:

> All Bank of America customers residing in New Jersey whose BOA consumer bank accounts were debited via one or more unauthorized transactions using Zelle and were not fully reimbursed by BOA.

118. Plaintiff SMITH is a member of and seeks to represent a Michigan state Sub-Class, pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), defined as:

> All Bank of America customers residing in Michigan whose BOA consumer bank accounts were debited via one or more unauthorized transactions using Zelle and were not fully reimbursed by BOA.

119. Excluded from the Nationwide Class and state Sub-Classes are Defendant's officers, directors, and employees; any entity in which Defendant have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant.

Further excluded from the Nationwide Class and state Sub-Classes are members of the judiciary to whom this case is assigned, their families, and members of their staff.

120. Plaintiffs reserve the right to modify the proposed class definitions, including but not limited to expanding the class to protect additional individuals and to assert additional sub-classes as warranted by additional investigation.

121. The proposed Nationwide Class and Sub-Classes meet the criteria for certification under Rule 23(a), (b)(2) and (b)(3).

122. **Numerosity:** The members of the Nationwide Class and Sub-Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, on information and belief, the Nationwide Class and Sub-Classes consists of thousands of individuals nationwide.

123. **Commonality:** There are questions of law and fact common to the Nationwide Class and Sub-Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation.

a. Whether Plaintiffs and the Class Members lost money that was unlawfully transferred from their account via Zelle;

b. Whether the transactions at issue were Unauthorized EFTs, by way of a third party fraudulently obtaining access to Plaintiffs' and the Class Members' accounts, making them errors subject to EFTA's remedial provisions, including Regulation E;

c. Whether Defendant violated EFTA by failing to adequately investigate the unauthorized transactions of Plaintiffs and the Class Members;

d. Whether Defendant limited its investigation to the payment instructions;

e. Whether Defendant violated EFTA by failing to provisionally credit the accounts of Plaintiff and the Class Members within 10 days of the transaction being disputed;

f. Whether Defendant violated EFTA by failing to correct errors on the accounts of Plaintiffs and the Class Members within 45 days of the transaction being disputed;

g. Whether Plaintiff and the Class Members are entitled to damages, including treble damages, maximum statutory damages, costs, fees and injunctive relief under the EFTA;

h. California Sub-Class: Whether the conduct of Defendant was "unlawful" as that term is defined in California's UCL;

i. California Sub-Class: Whether the conduct of Defendant was "unfair" as that term is defined in California's UCL;

j. California Sub-Class: Whether Defendant's advertising was untrue or misleading as those terms are defined in California's FAL;

k. South Carolina Sub-Class: Whether the conduct of Defendant was a "deceptive trade practice" as that term is defined in South Carolina's UTPA; and whether the Defendant breached a valid Contract with fraudulent intent;

l. New York Sub-Class: Whether the conduct of Defendant constitutes a deceptive act or practices and whether it constitutes false advertising as defined by N.Y. Gen. Bus. Law §§349, 350;

m. New Jersey Sub-Class: Whether the conduct of Defendant constitutes fraudulent or deceptive practices as defined by the New Jersey Consumer Fraud Act.

n. Michigan Sub-Class: Whether the conduct of Defendant constitutes a breach of contract and the implied covenant of good faith and fair dealing;

o. Whether Bank of America breached its contract with all Plaintiffs, and whether it breached the implied covenant of good faith and fair dealing;

p. Whether Plaintiffs and the respective Sub-Classes are entitled to damages, punitive damages, attorneys' fees, costs and injunctive relief under applicable state laws.

124. **Typicality**: Plaintiffs' claims are typical of those of other members of the Nationwide Class and Sub-Classes because Plaintiffs were victims of unauthorized transfers of funds from their BOA account, through the BOA/Zelle mobile app. After disputing that unauthorized transaction, Plaintiffs were informed by Defendant that the unauthorized transaction would not be reversed.

125. **Adequacy of Representation**: Plaintiffs will fairly and adequately represent and protect the interests of members of the Nationwide Class and Sub-Classes. Plaintiffs and their counsel have no conflicts of interest with the proposed Class and Sub-Classes. Plaintiffs' Counsel are competent and experienced in litigating consumer class actions.

126. **Predominance**: Defendant has engaged in a common course of conduct toward Plaintiffs as well as the members of the Nationwide Class and Sub-Classes, in that all were induced into using BOA's mobile app and online banking, that resulted in unauthorized withdrawals on their BOA accounts using Zelle. The common issues arising from Defendant's conduct affecting members of the Nationwide Class and Sub Classes set out above predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

127. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most members of the Nationwide Class and Sub-Classes would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual members of the Nationwide Class and Sub-Classes would create a risk of inconsistent or varying adjudications with

respect to individual members of the Nationwide Class and Sub-Classes, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

128. Defendant has acted on grounds that apply generally to the Nationwide Class and Sub-Classes, so that class certification is appropriate.

129. All Members of the proposed Nationwide Class and Sub-Classes are readily ascertainable. Defendant has access to consumer reporting of fraudulent and/or unauthorized transactions on their books and records, which they are required by law to maintain accurately. Using this information, Class Members easily can be identified and ascertained for the purpose of providing notice.

130. **Notice**: Plaintiffs anticipate providing direct notice to the members of the Nationwide Class and Sub-Classes for purposes of class certification, via U.S. Mail, email, and/or other electronic means, based upon Defendant's records.

## VII. CAUSES OF ACTION

### FIRST CAUSE OF ACTION

### The Electronic Fund Transfer Act ("EFTA")
### (On behalf of All Plaintiffs and the Nationwide Class)

131. Plaintiffs reallege and incorporate herein by reference the allegations contained in all preceding paragraphs, and further allege as follows:

132. The Electronic Fund Transfer Act ("EFTA") and Regulation E apply to electronic fund transfers that authorize a financial institution to debit or credit a consumer's account. 12 C.F.R. 100

133. The primary objective of EFTA is "the protection of individual consumers engaging in electronic fund transfers and remittance transfers." 12 C.F.R. § 1005.1(b).

156. Financial institutions have error resolution obligations pursuant to Regulation

E in the event that a consumer notifies the financial institution of an error. 12 C.F.R. § 1005.11.

134. Bank of America is a financial institution. 12 C.F.R. § 1005.2(i).

135. Pursuant to the EFTA, an error includes "an unauthorized electronic fund transfer." Id. § 1693f(f).

136. Electronic Fund Transfer ("EFT") is any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account. 12 C.F.R. 1005.3(b)(1). Accordingly, Regulation E applies to any P2P or mobile payment transactions that meet the definition of EFT. 12 C.R.F. 1005.3(b)(1)(v); id., Comment 3(b)(1)–1ii.

137. Unauthorized EFTs are EFTs from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit. 12 C.F.R. 1005.2(m).

138. According to the CFPB and FDIC, when a third party fraudulently induces a consumer into sharing account access information that is used to initiate an EFT from the consumer's account, that transfer meets Regulation E's definition of an unauthorized EFT. In particular, Comment 1005.2(m)–3 of Regulation E explains that an unauthorized EFT includes a transfer initiated by a person who obtained the access device from the consumer through robbery or fraud. As such, when a consumer is fraudulently induced into sharing account access information with a third party, and a third party uses that information to make an EFT from the consumer's account, the transfer is an unauthorized EFT under Regulation E.14.

139. Here, criminals used Plaintiffs and Nationwide Class Members BOA online account or mobile app to make unauthorized EFTs from Plaintiffs and Nationwide Class Members' BOA bank accounts.

140. After the unauthorized EFTs were made, the EFTs appeared on the bank statements of Plaintiffs and Nationwide Class Members.

141. Plaintiffs and Nationwide Class Members notified Defendant of these errors within sixty (60) days of their appearances on the accounts of Plaintiffs and Nationwide Class Members.

142. After receiving notice of the unauthorized EFTs on Plaintiffs' and other Nationwide Class Members' accounts, Defendant erroneously concluded that an unauthorized transfer did not occur.

143. A consumer's liability for an unauthorized transfer (or a series of related unauthorized transfers, 12 C.F.R. § 1005.6(b)), may not exceed $50. 15 U.S.C. § 1693g. Defendant violated the EFTA by holding Plaintiffs and Nationwide Class Members liable for unauthorized electronic funds transfers for more than $50. 15 U.S.C. § 1693g; § 1693m(a).

144. BOA did not make a good faith investigation of the alleged error and did not have a reasonable basis for believing that the consumer's account was not in error in violation of 15 U.S.C. § 1693f. Instead, BOA limited its "investigation" to the payment instructions.

145. BOA knowingly and willfully concluded that the Plaintiffs and Class members accounts were not in error when such conclusion could not reasonably have been drawn from the evidence available to the financial institution at the time of its investigation.

146. Defendant knowingly and willfully failed to fulfill their obligations to investigate Plaintiffs' unauthorized transactions and instead summarily concluded that the transfers of funds via Zelle on accounts of Plaintiffs and Nationwide Class Members were not in error when such conclusions could not reasonably have been drawn from the evidence available to the financial institutions at the time of the investigation. 15 U.S.C. § 1693f(e)(2).

147. Defendant's purported investigation is unlawful because Bank of America limits the investigation to the payment instructions; unlawfully places the burden of proof on the customer to prove a transfer was unauthorized; considers the customer's negligence in determining whether to reimburse an unauthorized transfer; treats claims involving Zelle

transfers different from other Electronic Funds Transfers; fails to review records from Zelle and/or from Network Banks; and knows specifically about the fraudulent schemes alleged, but still denies claims when consumers fall victim to those very schemes. It is not reasonable to limit the investigation to payment instructions when a consumer alleges their phone was stolen, their account was hacked, or was the result of similar fraud. Moreover, Plaintiffs allege additional facts that should be taken into account, including: that two Plaintiffs never used Zelle or enrolled in Zelle, and in certain instances the fraudster enrolled in Zelle and made the unauthorized transfer within seconds, and sent money to an account that Plaintiffs had no prior transactions with or connection. These factors—along with information about the identity or account history of the end recipient of the funds (which is information not available to Plaintiffs)—should have alerted the Bank that the disputed transactions were unauthorized.

148. Defendant did not investigate and determine whether an error has occurred and report or mail the results of such investigation and determination to the consumer within ten (10) business days. 15 U.S.C. § 1693f(a). BOA simply denied all claims based on the unauthorized payment instructions.

149. Defendant did not provisionally recredit the consumers' account ten days after receipt of notice of error to investigate, for the amount alleged to be in error pending an investigation. § 1693f(c). Instead, BOA unlawfully determined there was no error based solely on the payment instructions. Only after denying the claim, would BOA offer to investigate the claim in an effort to recover the funds, allowing itself another 45 days to investigate or recover the funds. Defendant employed this strategy to circumvent the EFTA's requirement to provisionally credit the consumer's account. By doing so, Defendant effectively allowed itself more than 10 days to investigate the claim without provisionally crediting the consumers account within 10 days, in violation of §1693f.

150. Defendant refused to completely reverse or refund funds to Plaintiffs and Nationwide Class Members consistent with their obligations under Regulation E, § 1005.6.

151. As a direct and proximate result of the conduct of the Bank, Plaintiffs and Nationwide Class Members were unable to reclaim funds that were fraudulently taken from their accounts within the authorized period for error resolution, and have been damaged thereby.

152. As such, Plaintiffs and Nationwide Class Members are each entitled to (i) actual damages sustained by the consumer; (ii) treble damages; (iii) the lesser of $500,000.00 or one percent (1%) of the net worth of BOA; (iii) reasonable attorneys' fees and costs; and (iv) injunctive relief to prohibit future unlawful conduct and compliance with the EFTA. 15 U.S.C. §§ 1693g; 1693f(e)(2), 1693m(a).

## SECOND CAUSE OF ACTION

### Breach of Contract
### (On Behalf of All Plaintiffs and CA, NY, NJ, SC, AND MI Sub-Classes)

153. Plaintiffs incorporate the preceding paragraphs of this Complaint as though fully stated herein.

154. Defendant and Plaintiffs entered into a valid Contract for online banking services.

155. Plaintiffs and Class Members contracted with BOA for checking account services, including mobile banking services, as embodied in the Agreement.

156. Defendant breached the Contract by failing to maintain the safety and security of Plaintiffs' and Class Members' online banking, and by holding Plaintiffs and Class Members liable for unauthorized Zelle transfers.

157. Plaintiffs suffered damages as a result of the breach of Contract, including the loss of money via unauthorized Zelle transfers, and any corresponding fees, interest, and charges.

## THIRD CAUSE OF ACTION

### Breach of the Implied Covenant of Good Faith and Fair Dealing (On Behalf of all Plaintiffs and CA, NY, NJ, SC, AND MI Sub-Classes)

158. Plaintiffs re-allege the paragraphs above as if fully set forth herein.

159. Plaintiffs and members of the Class contracted with BOA for checking account services, including mobile banking services, as embodied in the Online Banking Service Agreement.

160. This contract was subject to an implied covenant of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual duties—both explicit and fairly implied—and not to impair the rights of other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the covenant that Defendant would act fairly and in good faith in carrying out its contractual obligations to reimburse Plaintiffs and Class Members for unauthorized transactions if timely reported.

161. Defendant breached the implied covenant of good faith and fair dealing by: failing to maintain Plaintiffs and Class members accounts "safe" and "secure," failing to conduct a reasonable investigation of their claims, and holding Plaintiffs and Class Members liable for unauthorized transfers.

162. Specifically, the agreement states that "you will have no liability for unauthorized transactions if you notify us within 60 days after the statement showing the transaction has been sent to you."

163. Further, the contract states "We will determine whether an error occurred within 10 business days after we hear from you, and we will promptly correct any error we have made. If we need more time, however, we may take up to 45 days to investigate your complaint or question. In this case, we will provisionally credit your account within 10 business days for the amount you think is in error, so that you have the use of the money during the time it takes us to complete our investigation."

164. Moreover, the agreement specifically stated and implied that BOA's mobile banking was secure, that Plaintiffs and Class members would not be liable for unauthorized transactions, and that BOA would comply with the EFTA and Regulation E.

165. Nonetheless, BOA, in bad faith, intentionally breached this agreement by knowingly not maintaining a secure or safe service, creating policies to deny consumers legitimate claims for unauthorized transfers, failing to create policies and procedures to perform a reasonable investigation related to Zelle transfers, and refused to refund money for unauthorized transactions that were promptly reported by consumers. Moreover, BOA did not did not provisionally credit consumers' accounts while it was investigating the claim, as promised.

166. Each of Defendant's actions were done in bad faith and were arbitrary and capricious.

167. Plaintiffs and members of the Classes have performed all of the obligations imposed on the pursuant to the Online Banking Agreement.

168. Accordingly, Plaintiffs and Class Members have been injured as a result of Defendant's breach of contract and breach the covenant of good faith and fair dealing and are entitled to damages.

**FOURTH CAUSE OF ACTION**

**California's Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, et seq.**
**(On Behalf of Plaintiff Silverlight and California Sub-Class)**

169. Plaintiffs reallege and incorporate herein by reference the allegations contained in all preceding paragraphs, and further allege as

follows:

170. The UCL defines "unfair business competition" to include any "unlawful, unfair, or fraudulent" act or practice, as well as any "unfair, deceptive, untrue or misleading" advertising. Cal. Bus. & Prof. Code § 17200.

171. The UCL imposes strict liability. Plaintiffs need not prove that Defendant intentionally or negligently engaged in unlawful, unfair, or fraudulent business practices—but only that such practices occurred.

**"Deceptive Prong"**

172. A business act or practice is "fraudulent" under the UCL if it is likely to deceive members of the public. Defendant's practices, as described herein, constitute "fraudulent" business practices in violation of the UCL because, among other things, Defendant Bank of America's marketing regarding its online banking and Zelle services states the Bank will protect against, and guarantees no liability for, unauthorized transfers.

173. Defendant also concealed the security risks of using the Bank of America online banking and mobile app after integrating the Zelle service, including the risk of fraud and the risk that criminals will target them and that they will not be reimbursed by BOA as a matter of practice, which is a practice that is likely to deceive a consumer acting reasonably under the circumstances, to the consumer's detriment.

**"Unfair" Prong**

174. A business practice is "unfair" under the UCL if it offends an established public policy or is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers, and that unfairness is determined by weighing the reasons, justifications and motives of the practices against the gravity of the harm to the alleged victims.

175. Defendant's actions constitute "unfair" business practices because, as alleged above, they declined to reverse fraudulent charges on the accounts of Plaintiff Silverlight and California Sub-Class Members, despite marketing representations, contract promises, and statutory obligations pursuant to EFTA.

176. The harm to Plaintiff Silverlight and California Sub-Class Members grossly outweighs the utility of Defendant's practices as there is no utility to the practices of Defendant.

**"Unlawful" Prong**

177. A business act or practice is "unlawful" under the UCL if it violates any other law or regulation.

178. Defendant's acts and practices alleged above constitute unlawful business acts or practices as they have violated the plain language of EFTA as described in Plaintiffs' First Cause of

Action above. The violation of any law constitutes as "unlawful" business practice under the UCL.

179. These acts and practices alleged were intended to or did result in violations of EFTA and Regulation E.

180. Defendant has and will continue to unlawfully deny the transaction disputes of Plaintiff Silverlight and the California Sub-Class, and the public by claiming that said disputed transactions are "authorized," even though said transactions are actually "unauthorized," as that term is defined by EFTA and applicable regulations. Consequently, the practices of BOA constitute fraudulent, unfair and unlawful business practices within the meaning of the UCL.

181. Pursuant to the UCL, Plaintiff Silverlight and the California Sub-Class do not have an adequate remedy at law and are entitled to preliminary and permanent injunctive relief and an order requiring Defendant to cease this unfair and unlawful competition, as well as disgorgement and restitution to Plaintiff and the California Sub-Class of all revenues associated with this unfair and unlawful competition, or such portion of said revenues as the Court may find applicable.

## FIFTH CAUSE OF ACTION

### California's False Advertising Law, Cal. Bus. & Prof. Code §§ 17500, Et. Seq. (Asserted on Behalf of Plaintiff Silverlight and California Sub-Class)

182. Plaintiffs repeat and reallege the above allegations as if fully set forth her California's False Advertising Law ("FAL"), Cal. Bus. & Prof. Code § 17500, states that "[i]t is unlawful for any ... corporation ... with intent ... to dispose of ...personal property ... to induce the public to enter into any obligation relating thereto, to make or disseminate or cause to be made or disseminated ... from this state before the public in any state, in any newspaper or other publication, or any advertising device, or by public outcry or proclamation, or in any other manner or means whatever, including over the Internet, any statement...which is untrue or

misleading and which is known, or which by the exercise of reasonable care should be known, to be untrue or misleading....”

183. Defendant’s material misrepresentations and omissions alleged herein violate Bus. & Prof. Code § 17500.

184. Defendant knew or should have known that their misrepresentations and omissions were false, deceptive, and misleading.

185. Pursuant to Business & Professions Code §§ 17203 and 17500, Plaintiff and the members of the California Sub-Class, on behalf of the general public, seek an order of this Court enjoining Defendant from continuing to engage, use, or employ their practice of misrepresenting the online banking and Zelle service.

186. Further, Plaintiff and the members of the California Sub-Class seek an order requiring Defendant to disclose such misrepresentations, and additionally request an order awarding restitution of the money wrongfully acquired by Defendant by means of said misrepresentations.

187. Additionally, Plaintiff and the members of the California Sub-Class seek an order requiring Defendant to pay attorneys’ fees pursuant to Cal. Civ. Code § 1021.5.

**SIXTH CAUSE OF ACITON**

**South Carolina Unfair Trade Practices Act, S.C. Code §39-5-10, et. Seq.**
**(On behalf of Plaintiff Georgion and South Carolina Sub-Class)**

188. Plaintiffs incorporate by reference all preceding paragraphs of this Complaint as if fully set forth herein.

189. Defendant is a “person” under S.C. Code Ann. § 39-5-10.

190. The activities of Defendant described herein constitute “trade or commerce” as defined by South Carolina Code Section 39-5-10, et seq.

191. The South Carolina Unfair Trade Practices Act (“UTPA”) prohibits “unfair or deceptive acts or practices in the conduct of any trade or commerce.” S.C. Code Ann. § 39-5- 20(a).

192. Defendant's actions, statements, and omissions had the capacity or tendency to deceive and mislead. The Plaintiff suffered actual damages as a result of Defendant's conduct.

193. Upon information and belief, Defendant has repeated and is repeating this conduct throughout the state of South Carolina.

194. Defendant's employment of the aforesaid deceptive practices and acts was a willing and knowing violation.

195. Plaintiff Georgion and South Carolina Sub-Class Members seek actual damages, treble damages, attorney fees and costs. S.C. Code 39-5-140.

**SEVENTH CAUSE OF ACTION**

**Breach of Contract With Fraudulent Intent**
**(On behalf of Plaintiff Georgion and South Carolina Sub-Class)**

196. Defendant and Plaintiff Georgion entered into a valid and enforceable Agreement for online banking and mobile banking services.

197. Defendant breached that Agreement.

198. Plaintiff and Class Members suffered damages as result of the breach of contract.

199. Defendant breached the contract with fraudulent intent accompanied by fraudulent acts. "The fraudulent act element is met by any act characterized by dishonesty in fact, unfair dealing, or the unlawful appropriation of another's property by design." *Perry v. Green*, 313 S.C. 250, 254, 437 S.E.2d 150, 152 (Ct. App. 1993).

200. Defendant knowingly and intentionally violated the Contract and acted unfairly in the following ways:

a. Defendant told Plaintiff and Class Members that their unauthorized Zelle transfer would not be refunded in violation of the Contract and Federal Law;

b. Defendant created policies and procedures to deny the claims for unauthorized transfers and to hold the Plaintiff and Class Members liable in violation of the Contract;

c. Defendant intentionally failed to provisionally credit consumers accounts;

d. Defendant knew that incorporating Zelle into the online banking and mobile app created security risks for their customers and subject to the financial harm, and did so anyways, in violation of the Contract.

201. Plaintiff and Class Members suffered damages as a result of and seeks actual and punitive damages.

## EIGHTH CAUSE OF ACTION

### New York Consumer Fraud Act, NYGBL § 349, et seq.
### (On behalf of Plaintiff Purdy and New York Sub-Class)

202. Plaintiff repeats and realleges the above allegations as if fully set forth herein.

203. This cause of action is brought under New York's General Business Law § 349, et seq. 143. N.Y. Gen. Bus. Law § 349(a) provides that "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

204. Defendant committed deceptive acts and practices in violation of N.Y. Gen. Bus. Law 349 by failing to disclose material facts regarding the true risks of using the BOA online banking and mobile banking service, by failing to disclose material facts regarding the true risks of Zelle, and failing to refund consumers for unauthorized Zelle transfers despite its promises.

205. Defendant's actions and omissions regarding its Online Banking and Mobile Banking service, and its Zelle money transfer service, as described herein, are deceptive acts or practices in the conduct of business trade or commerce of goods.

206. As described herein, BOA advertisements that its services were safe and secure constitutes deceptive acts or practices in the conduct of business trade or commerce in violation of N.Y. Gen. Bus. Law § 349.

207. As described herein, Defendant's misrepresentations that it will protect accountholders who incur unauthorized transfers, constitutes deceptive acts or practices in the conduct of business trade or commerce in violation of N.Y. Gen. Bus. Law § 349.

208. Defendant's deceptive omission of the material security risks of using the online or mobile banking service and the Zelle service, including the risk of fraud and the risk that fraudulent losses will never be reimbursed by BOA, is a practice that is likely to mislead a consumer acting reasonably under the circumstances.

209. The deceptive acts and practices and the conduct of business trade or commerce of goods took place in New York.

210. N.Y. Gen. Bus. Law § 349(h) provides that "any person who has been injured by reason of any violation of this section may bring an action in his own name to enjoin such unlawful act or practice, an action to recover his actual damages or fifty dollars, whichever is greater, or both such actions.

211. As a direct and proximate result of Defendant's misconduct, Plaintiff and members of the New York Class were injured and suffered actual damages.

## NINTH CAUSE OF ACTION

### Violation of New York GBL §350
### (On behalf of Plaintiff Purdy and New York Sub-Class)

212. Plaintiff repeats and realleges each and every allegation contained in all the foregoing paragraphs as if fully set forth herein.

213. N.Y. Gen. Bus. Law § 350 provides that false advertising in the conduct of any business, trade or commerce or in the furnishing of any service in this state is hereby declared unlawful. N.Y. Gen. Bus. Law § 350a(1).

214. Defendant's labeling and advertisements contain untrue and materially misleading statements concerning Defendant's Online and Mobile Banking Services as they misrepresent that they are safe, secure, and that customers will not be liable for unauthorized transactions.

215. Defendant knowingly and willfully made these false advertisements in violation of New York law.

216. Plaintiff and class members suffered damages as a result of the deceptive acts and practices.

## TENTH CAUSE OF ACTION

### Violation of New Jersey's Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2 (On behalf of Plaintiff Williams and New Jersey Sub-Class)

217. Plaintiffs repeat and reallege each and every allegation contained in all the foregoing paragraphs as if fully set forth herein.

218. The New Jersey Consumer Fraud Act ("NJCFA") makes unlawful "[t]he act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate … is declared to be an unlawful practice." N.J. Stat. Ann. § 56:8-2.

219. Defendant's practices, as described herein, constitute an unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact, with respect to the advertisement of their online and mobile banking service utilized by Plaintiff and New Jersey Class members, in violation of the NJCFA, including by knowingly and intentionally making false or misleading representations that its online and mobile banking was "safe" and "secure", that Zelle was safe and secure, and that BOA customers would not be held liable for unauthorized transactions.

220. Defendant, as described herein, violated the NJCFA, by knowingly and intentionally concealing and failing to disclose material facts regarding the true risks of utilizing the mobile and online banking service and the Zelle money transfer service through its website and mobile app.

221. Defendant's practices, as described herein, constitute deceptive and/or fraudulent business practices in violation of the NJCFA because, among other things, they are likely to deceive reasonable consumers, who expect their bank to protect their money.

222. Moreover, Defendant's willful and intentional concealment and omission of the security risks of using the online or mobile banking service, including the risks associated with Zelle, and the risk that unauthorized transactions via Zelle will not be reimbursed, is a practice that is likely to deceive a consumer acting reasonably under the circumstances, to the consumer's detriment.

223. Defendant committed deceptive and fraudulent business acts and practices in violation of the NJCFA, by affirmatively and knowingly misrepresenting on its website and mobile app the true risks and operation of its service.

224. As a direct and proximate result of Defendant's deceptive and fraudulent business practices, Plaintiff Williams and New Jersey Class members have suffered an ascertainable loss and actual damages.

225. Defendant's fraudulent conduct is ongoing and presents a continuing threat to New Jersey Class members.

226. Plaintiff and New Jersey Class members seek an order enjoining Defendant's unfair and deceptive acts or practices in violation of the NJCFA and awarding actual damages, treble damages, costs, attorneys' fees, and any other just and proper relief available under the NJCFA.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for relief in this Complaint as follows:

- For actual damages;
- For an award of statutory damages;
- For an award of treble damages;
- For an award of punitive damages;

- For prejudgment interest;
- For an award of injunctive relief;
- For an award of attorney fees;
- For an award of costs; and,
- For any and all other relief the Court deems just and appropriate.

Plaintiffs hereby demand a jury trial on all issues so triable.

Respectfully submitted,

LAW OFFICES OF ANDREW J. BROWN

s/ *Andrew J. Brown*
Andrew J. Brown
Brian J. Ellsworth
501 West Broadway, Suite 1490
San Diego, CA 92101
Telephone; (619) 501-6550
andrewb@thebrownlawfirm.com
briane@thebrownlawfirm.com

*Attorneys for Plaintiffs on behalf of themselves, and all others similarly situated*

BLOSSOM LAW PLLC

Rashad Blossom
301 S. McDowell Street, Ste. 1103
Charlotte, NC 28204
(704) 256-7766

*Local Counsel for Plaintiffs*